ISSN 0974-3618 (Print) **www.rjptonline.org**
0974-360X (Online)

RESEARCH ARTICLE

A Tree Structure Based Key Generation Technique for Data Security Enhancement

G. Manikandan*, P. Rajendiran, V. Harish, Nooka Sai Kumar
Department of Information and Communication Technology, School of Computing, SASTRA University,
Thanjavur – 613401, Dist – Thanjavur (T.N) India.
*Corresponding Author E-mail: **manikandan@it.sastra.edu**

ABSTRACT:
Information Security is an important issue of concern in communicating the data between the parties. Cryptographic algorithms emerged as a solution and have contributed a major role in information security system. Most of the cryptographic algorithms rely on a key for performing encryption and decryption. The key used along with the algorithm plays a vital role in ensuring the security and confidentiality of the text that is transmitted. In this work, we propose a new technique to generate a new key from the given key using different tree structures. If the key size is less than 128 bits, the given key is converted to 56 bits and then the given text is encrypted with DES followed by Blowfish algorithm. If the key size is greater than 127 bits, the given key is converted to 128 bits and then the given text is encrypted with AES followed by the RC6 algorithm. The reverse process is carried out for decryption in both the cases.

KEYWORDS: AES, DES, Blowfish, RC6, AVL, BST.

INTRODUCTION:

Cryptography is an art of science that deals with ciphering and deciphering the data. Two kinds of keys namely Symmetric and Asymmetric keys, are used during the encryption and decryption process. In Symmetric Key Cryptography, a single shared key is used for both encryption and decryption phases. The sender to encrypts the plaintext using the key and transmits the ciphertext to the receiver. The receiver uses the same key to recover the plaintext from the ciphertext. Asymmetric key cryptography makes use of a key pair, (i.e.) a public key and a private key. Both the keys are a must for ciphering and deciphering the data. The private key is the key which is known only to the person who encrypts or decrypts and it is unsharable. To increase the complexity a new key is generated from the given key. For generating the new key tree structures like AVL, BST and Binary trees are used.

Received on 19.07.2017 Modified on 09.08.2017
Accepted on 20.08.2017 © RJPT All right reserved
Research J. Pharm. and Tech. 2017; 10(9): 2895-2898.
DOI: 10.5958/0974-360X.2017.00511.X

Cryptographic algorithms like AES algorithm, DES algorithm, Blowfish algorithm, the RC6 algorithm is used for the encryption and decryption of the message. The Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are Symmetric key block ciphers. AES uses 128-bit data with a 128/192/256-bit key. DES has an effective key length of 56 bits and uses 16 round Feistel structure. Blowfish algorithm has a 64-bit block size with a variable key length ranging from 32 bits up to 448 bits. RC6 is a 64-bit block cipher with a variable key size using 18 rounds.

MATERIAL AND METHODS:

This work mainly concentrates on increasing the complexity of the key used in the cryptographic algorithm, which increases the complexity for the intruders. A tree structure based key technique is used to maintain the integrity and confidentiality of the data transmitted.

Key generation using trees:

For the shared key, three trees are constructed using tree structures like AVL, BST and Binary trees. The first step in this process is to generate the trees for the given key. Then it is used to assign a unique code to each character in the given key. Starting from the root, ‘0’ is assigned to the left branch and ‘1’ to the right branch and the pattern is repeated for each node in the tree. A character’s code can be found by traversing from the root and following the branches that lead to the character.

For the given key value ABCDEFG, as shown in the fig.1, the modified keys Generated from the tree by traversing it using different tree structures are shown below.

Binary Tree – 00001000001010011
BST – 00001000001010011
AVL Tree- 00000001001001011

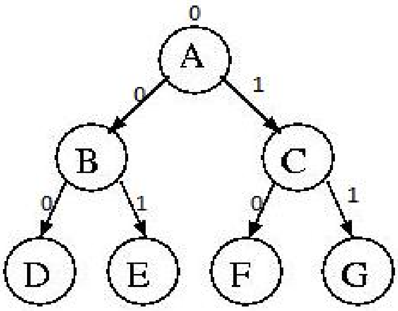

Fig 1: Tree Structure for the given key

The key generated from the trees are stored in an array in a different combination of the three keys. Since 3 keys are obtained from three trees we get 3! (i.e.) 6 combinations of keys generated and stored in that array as shown in table 1. From this array only one key is chosen for the encryption and decryption process.

Table 1 – Table representing array of keys

Index	Stored Key
0	000010000010100110000000100100101100001000001010011
1	000010000010100110000100000101001100000001001001011
2	000000010010010110000100000101001100001000001010011
3	000000010010010110000100000101001100001000001010011
4	000010000010100110000100000101001100000001001001011
5	000010000010100110000000100100101100001000001010011

Steps for choosing the key from the array:

1: Calculate key length

Total length=key length (AVL) +key length (BST) +key length (Binary Tree) = 17+17+17 =51

2: Finding the index value

Index=Total length % 6 = 51 % 6 = 3

3: Select the key based on the index obtained. Thus the key is

000000010010010110000100000101001100001000001010011.

Working of Algorithm:

Once the key is generated it is used in a different encryption algorithm to encrypt the text. In this proposed model, 4 algorithms are used. They are AES algorithm, DES Algorithm, Blowfish Algorithm, RC6 algorithm.

Here in encrypting and decrypting the data two procedures are followed.

1) If the key size is less than 128 bits, then DES followed by Blowfish algorithm is performed to encrypt and decrypt the text.
2) If the key size is greater than 127 bits, then AES followed by the RC6 algorithm is performed to encrypt and decrypt the text.

The steps involved in the proposed system are shown diagrammatically in figure 2 and 3.

Module 1:

Encryption:

If the key size is lesser than 127 bits then the key generated using the three trees is passed as a seed value to the DES algorithm and that key is converted into the 56-bit key and the text is encrypted using this key and the plain text is converted into ciphertext. Then obtained cipher text is again encrypted using Blowfish Algorithm using the same key. After this two encryption process, the obtained cipher text is transmitted through the network.

Decryption:

Key generation is quite similar to the encryption process. The order of the encryption process is reversed for the decryption process. First the data is decrypted by Blowfish algorithm and the obtained text from Blowfish is decrypted by DES algorithm to get the original plain text.

Module2:

Encryption:

If the key size is greater than 127 then the key generated using the three trees is passed as a seed value to the AES algorithm and that key is converted into the 128-bit key and the text is encrypted using this key and the plain text is converted into ciphertext. Then obtained cipher text is again encrypted using RC6 algorithm using the same key. After this encryption process the obtained cipher text is transmitted through the network.

Decryption:

Key generation is quite similar to the encryption process. Decryption takes place in the reverse order of ciphering phase. First the data is decrypted by the RC6 algorithm then by AES algorithm to get the original plain text.

Pseudo code for encryption side:

- A key is shared between sender and receiver.
- Using the key shared, three new keys are generated using three tree algorithms.
- A total of 3! Key combinations are generated and stored in an array.
- From the array one key is chosen by Key index=length (AVL key + Binary Tree key + BST key) % 6
- If the key size is < 128 then 56-bit encryption algorithm is used to encrypt the plain text (here DES and Blowfish algorithm). The cipher text is produced after encryption.
- If the key size is > 127 then 128-bit encryption algorithm is used to encrypt the plain text (here AES, RC6). The cipher text is produced after encryption.

Pseudo code for decryption side:

- Using the key shared, three new keys are generated using three tree algorithms.
- A total of 3! Key combinations are generated and stored in an array.
- From the array one key is chosen by

Key index=length (AVL key + Binary Tree key + BST key) % 6

- If the key size is < 128 then 56-bit decryption algorithm is carried out to decrypt the cipher text (Blowfish algorithm and DES). The plain text is produced after decryption.
- If the key size is > 127 then 128-bit decryption algorithm is carried out to decrypt the cipher text (RC6 and AES). The plain text is produced after decryption.

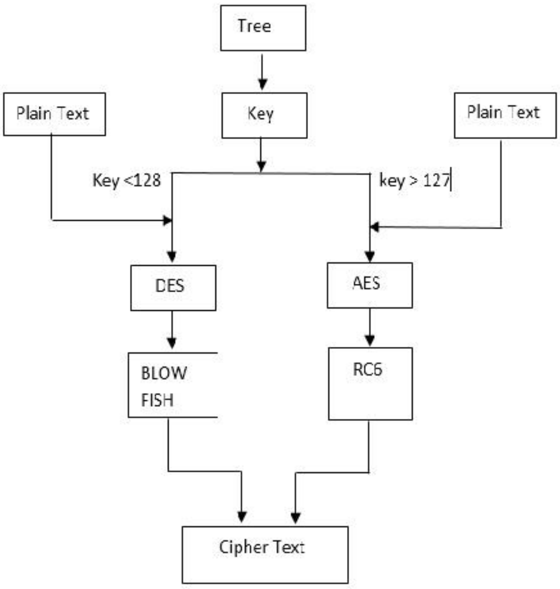

Fig 2: Steps in the Encryption process

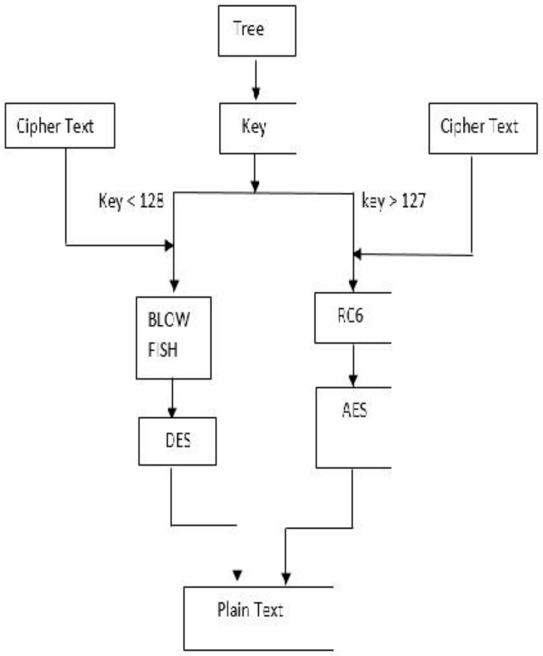

Fig 3: Steps in the Decryption process

RESULTS AND DISCUSSION:

Even though the attackers get the knowledge of the key that is shared initially, it is not possible to infer the new key generated by the proposed system which proves to be the novelty of this work. In this model the key is also encrypted (i.e.) initially a key is shared between the users and the contents of that key is converted into binary bits using a separate tree structure-based mechanism and this newly created key is used for encryption. The binary equivalent of a particular character depends according to its position in the tree whereas the bit representation of a character remains the same in the traditional case. In this way the proposed model increases the confidentiality of the message, as well as the complexity of finding the actual key by the intruders is also increased.

ACKNOWLEDGEMENT:

The authors would like to thank the Department of Science and Technology, India for their financial support through Fund for Improvement of S&T Infrastructure (FIST) programme SR/FST/ETI-349/2013.

CONFLICT OF INTEREST:

The authors declare no conflict of interest.

REFERENCES:

1. G. Manikandan, R. Manikandan, G. Sundarganesh. A New Approach for Generating Strong Key in RC4 Algorithm. Journal of Theoretical and applied information Technology. 2011. 24; 113-119.
2. V. Vaithiyanathan, G. Manikandan, G. Krishnan. A Novel

Approach to the Performance and Security Enhancement Using Blowfish Algorithm. International Journal of Advanced Research in Computer Science. 2010. 1; 451-454.

3. Dr. N. Sairam, G. Manikandan, G. Krishnan. A Novel Approach for Data Security Enhancement Using Multi Level Encryption Scheme. International Journal of Computer Science and Information Technologies. 2011. 2; 469-473.
4. G. Manikandan, R. Manikandan, P. Rajendiran, G. Krishnan, G. Sundarganesh. An Integrated Block and Stream Cipher Approach for Key Enhancement. Journal of Theoretical and applied information Technology. 2011. 28; 83-87.
5. G. Manikandan, G. Krishnan, Dr. N. Sairam. A Unified Block and Stream Cipher Based File Encryption. Journal of Global Research in Computer Science. 2011. 2; 53-57.
6. G. Manikandan, M. Kamarasan, P. Rajendiran, R. Manikandan. A Hybrid Approach for Security Enhancement by modified Crypto-Stegno scheme in European. Journal of Scientific Research. 2011. 60; 224 – 230.
7. G. Manikandan, P. Rajendiran, K. Chakarapani, G. Krishnan, G. Sundar Ganesh. A Modified Crypto Scheme for Enhancing Data Security. Journal of Theoretical and applied information Technology. 2012. 35; 149-154.
8. G. Manikandan, N. Sairam, M. Kamarasan. A New Approach for Improving Data Security Using Iterative Blowfish Algorithm. Journal of Applied Sciences, Engineering and Technology. 2012. 4; 603-607.
9. G. Manikandan, N. Sairam, M. Kamarasan. A Hybrid Approach for Security Enhancement by Compressed Crypto-Stegno Scheme. Journal of Applied Sciences, Engineering and Technology. 2012. 4; 608-614.
10. S. Karthikeyan, N. Sairam, G. Manikandan, J. Sivaguru. A Parallel Approach for Improving Data Security. Journal of Theoretical and Applied Information Technology. 2012. 39; 119-125.
11. S. Karthikeyan, N. Sairam, G. Manikandan. A New Approach for Enhancing Data Security Using Parallel Processing. Advances in Natural and Applied Sciences. 2012. 6; 696-703.
12. G. Manikandan, R. Dalhouse Prabu, P. Sravan Kumar, M. Sudhakar Raj, S. Venkatakrishnan. Rendering A Fortify Key to Enhance the Security of Cryptographic Algorithms. International Journal of Applied Engineering Research. 2014. 9; 1987-1955.
13. P. L. Sharma, M. Rehan. Modified Hill Cipher Using Vandermonde Matrix and Finite Field. Int. J. Tech. 4(1): Jan.-June. 2014; Page 252-256
14. Satish Garg, Priyanka Vaishist, S. P. Gupta. Data Security by Hide and Retrieval Method Using Rotation Cipher. Int. J. Tech. 2016; 6(2): 59-62.
15. Satish Kumar Garg. Data Security Using Triple Encryption. Int. J. Tech. 2016; 6(2):206-208.
16. A. Manimaran, V. M. Chandrasekaran, Arnav Bhutani, Vansh Badkul. A New Approach for Encryption and Decryption. Research J. Pharm. and Tech. 2016; 9(12)2322-2326.
17. Satish Kumar Garg. Cryptography Using Xor Cipher. Research J. Science and Tech. 2017; 9(1):25-28.
18. Satish Kumar Garg. Cryptography Using Transposition Cipher. Research J. Science and Tech. 2017; 9(1):48-50.
19. Rajdeep Chowdhury, Saikat Ghosh. Study of Cryptology Based on Proposed Concept of Cyclic Cryptography Using Cyclograph. Research J. Engineering and Tech. 2(1): Jan.-Mar. 2011 page 17-20.
20. Narendra K. Dewangan, Manisha Dewangan. Image Encryption and Decryption Using Auto Generated Key. Research J. Engineering and Tech. 2(4): Oct. - Dec. 2011 page 219-222.
21. Narendra Kumar Dewanga, Nilmani Verma, Sandeep Gonnade. Digital Image Security using Auto Key Generation with Segmentation. Int. J. Tech. 3(1): Jan.-June. 2013; Page 15-18
22. Sulakshana Bhariya, Guide Jagveer Verma. A Bio-Cryptography Approach for Improving the Security of Image Encryption and Decryption. Int. J. Tech. 2(1): Jan.-June. 2012; Page 17-20